

# Exhibit 6

Ex. 6:

Firefox • ATEN Intern. Co. Ltd. v. Emine... • Technicolor works hard at sto... •

blog.apex.aero/content-2/technicolor-works-hard-stopping-hackers-stealing-ife-content/

### Technicolor works hard at stopping hackers from stealing IFE content

September 25, 2012 Content



As technology continues to progress and hackers continue to hack, it's no surprise that professionals like Eric Diehl, VP of security systems & technology and business security services at Technicolor, are becoming evermore vigilant about ensuring that appropriate security protocols are in place to protect entertainment content.

"One of the biggest things that I am seeing today is BYOD (Bring Your Own Device). Now everyone is advocating it, as soon as you open that door you open it to the bad guys, the hackers," says Diehl.

At Technicolor's Security & Content Protection laboratories, where Diehl works with a team of 30 international security experts, the mission is to research the content solutions of the future, secure products and services, and evaluate their level of security.

Encryption and watermarking is used to protect data in transit. With leakage of early content being the studios' and airlines' main concerns, the security goals that Diehl proposes are tracing the source and controlling the usage of the content. "It's about creating new concepts, systems, and designing them."

So what exactly does this system mean for IFE? "Technicolor's ContentArmor solution sends the same encrypted content to all receivers. Each authorized receiver decrypts the encrypted content, embeds invisible and invisible watermarks unique to the receiver and adds visible marks. It offers high security and individual forensic marking while simplifying the logistics and content preparation," explains Diehl.

Oliver de Courson, VP of media services sales at Technicolor, notes that "the overarching premise for IFE is driven by early window movies. That is why the security is so important. We protect the studios as content providers. We protect IFE and the business proposal."

Adds Diehl: "What IFE is facing now is something we've been facing for three, five years in the Set Top Box and gateway market. Now that it's open to the Internet, we're facing exactly the same problem."

Knowing that "hackers always find a way," Diehl's team says it has become a challenge fighting "the bad guys".

"It's a constant evolving challenge," notes Courson, "but we constantly stay ahead."

Diehl recently gave a security presentation at the Technology Committee gathering in Burbank, and was then asked by APEX to present at this year's EVPO, which he did last week. "Based on the fact of how highly received it was," explains Bryan Rusenko, VP of strategy & technology, IFE at Technicolor, he (Diehl) was asked to speak at this conference. "Both of Diehl's presentations have generated great interest to the airlines and IFE distribution companies."

Share / Save

byod, content, contentarmor, hackers, ife, inflight entertainment, mobiles, passenger, peds, security, technicolor, wireless ife

Next Previous Highlight all Match case

APEX eMagazines



Managed content



amp International



Connect with APEX



Revolutionizing in-Flight Entertainment



AirFlix



JAGUAR



ALEX CROSS

